# Hillstone Unified Intelligence Firewall Installation Manual

www.hillstonenet.com

# Preface

## Conventions

This document follows the conventions below:

### Content

- **Tip**: provides reference.
- **Note**: indicates important instructions for you better understanding, or cautions for possible system failure.
- Bold font: indicates links, tags, buttons, checkboxes, text boxes, or options. For example, "Click **Login** to log into the homepage of the Hillstone device", or "Select **Objects** > **Address Book** from the menu bar".
- When clicking objects (menu, sub-menu, button, link, etc.) on WebUI, the objects are separated by an angled bracket (>).

### CLI

- Braces ({ }): indicate a required element.
- Square brackets ([ ]): indicate an optional element.
- Vertical bar (|): separates multiple mutually exclusive options.
- **`Bold`**: indicates an essential keyword in the command. You must enter this part correctly.
- *`Italic`*: indicates a user-specified parameter.
- The command examples may vary from different platforms.
- In the command examples, the hostname in the prompt is referred to as host-name.

# Table of Contents

**Chapter 1 Overview ..... 1**

**Chapter 2 Prerequisite ..... 3**

*Virtual Machine ..... 3*

*Unified Intelligence System Software ..... 4*

*Hillstone Device, Firmware, and License ..... 5*

*Routing Requirements ..... 6*

**Chapter 3 Installation and Upgrading ..... 8**

*Installing Unified Intelligence System Software ..... 10*

*Upgrading Hillstone Device ..... 16*

**Chapter 4 Initialization ..... 18**

*Works Executed in Virtual Machine ..... 18*

*Works Executed in Hillstone Device ..... 20*

Via WebUI ..... 20

Via CLI ..... 21

**Chapter 5 Logging into Unified Intelligence Firewall ..... 23**

**Chapter 6 Advanced Settings ..... 24**

*Showing Interface Information ..... 24*

*Configuring Interface Settings ..... 24*

*Modifying Login Password ..... 24*

*Upgrading Unified Intelligence Firewall ..... 24*

Via WebUI ..... 24

Via CLI ..... 26

*Upgrading/Rolling Back Firmware of Hillstone Device ..... 26*

*Deleting Unified Intelligence System ..... 27*

*Showing Version Information ..... 27*

*Configuring Trusted Hosts ..... 27*

*Securing Communication between Unified Intelligence System and Hillstone Device ..... 27*

*Viewing Share Keys ..... 28*

*Clearing Share Keys ..... 28*

**Copyright Information ..... 29**

# Chapter 1 Overview

Hillstone unified intelligence firewall consists of the following two parts:

- Virtual machine + unified intelligence system software: Install the unified intelligence system software in the virtual machine that meets the requirements. The virtual machine with the unified intelligence system software installed is a unified intelligence system. The unified intelligence system has the functions of data storing, data mining and analyzing, etc.
- Hillstone device: Upgrade the Hillstone device to the specified firmware. The upgraded Hillstone devices have the functions of date forwarding, threat detection, etc. For information about the product models that support the firmware upgrading, see Table 1.

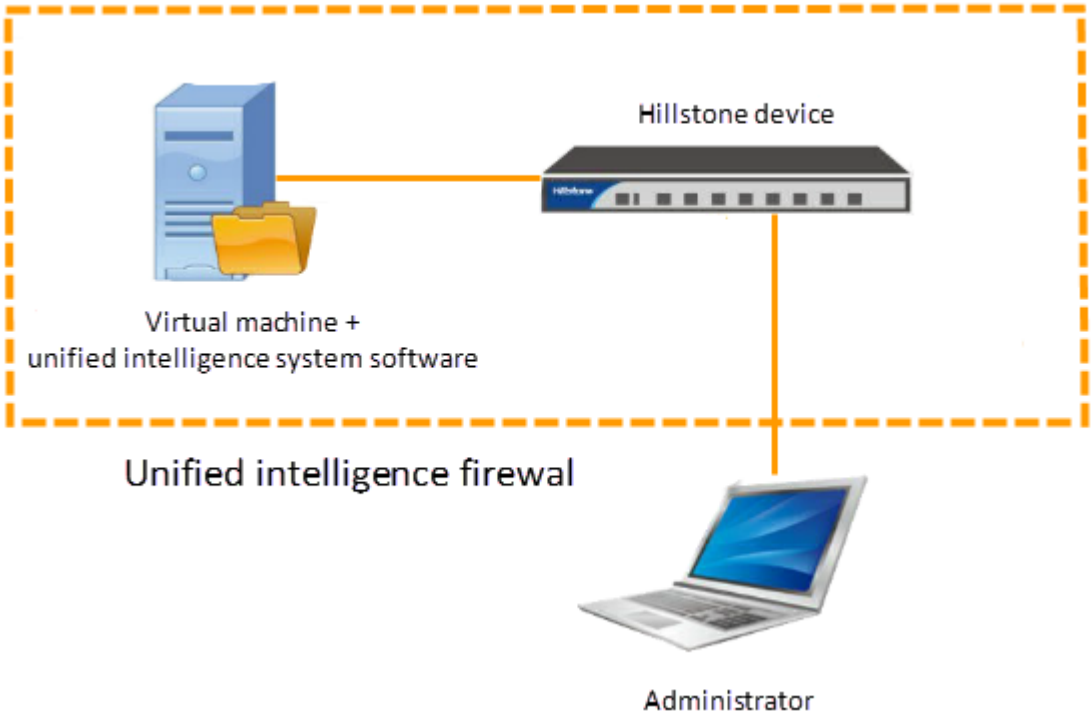


**Figure 1:** Consisting of Two Parts

Hillstone devices that support the unified intelligence firewall are listed in the table below. The Hillstone devices are categorized since requirements of virtual machines for each Hillstone device category are different.

| Category | Product Model |
|---|---|
| A | M1600, M2600, M3600, M2105, M3100, M3105, M3108、E1600、E1700 |
| B | M6110, M6115, G2110, G2120、E2300、E2800 |

| Category | Product Model |
|---|---|
| C | G3150, G5150, M6560, M6860, G6100、E3660、E3960、E5260 |
| D | X5100, M7260, M7360, M7860, M8260, M8860、E5560、E5660、E5760、E5960 |

**Table 1:** Product Models and Categories

# Chapter 2 Prerequisite

To use the unified intelligence firewall, ensure the following prerequisites.

- Virtual machine. For more information, see Virtual Machine.
- Unified intelligence system software. For more information, see Unified Intelligence System Software.
- Hillstone device, the firmware for upgrading Hillstone device, and license for unified intelligence service. For more information, see Hillstone Device, Firmware, and License.
- Routing between the virtual machine and the Hillstone device is reachable. For more information, see Routing Requirements.

The following sections describe the above four prerequisites.

## Virtual Machine

For each category of Hillstone devices, the recommended hardware parameters of the virtual machine are different. Make sure the hardware parameters of the virtual machine meet the requirements described in Table 2 and make sure the PC or server meets the requirements described in Table 3. In Table 3, the value recommended in the Memory parameter is calculated by adding the following two parts:

- 4 GB needed by the program of VMware vSphere Hypervisor
- The memory needed by the unified intelligence system software. The memory for each category of Hillstone devices is different.

When creating a virtual machine, use VMware vSphere Hypervisor whose version is higher than 5.0. For more information about account register and software downloading, visit https://my.vmware.com/cn/web/vmware/login.

For more information about virtualization support by Intel, visit http://ark.intel.com/Products/VirtualizationTechnology.

| Category | Recommended Hardware Parameters | | | Bandwidth between Virtual Machine and Hillstone Device (Mbps) |
|---|---|---|---|---|
| | CPU | Memory (GB) | Hardware Disk (GB) | |
| A | 4 cores * 0.8 GHz | 4 | 160 | 80 |
| B | 4 cores * 1.2 GHz | 6 | 280 | 160 |
| C | 4 cores * 2.5 GHz | 10 | 450 | 400 |
| D | 4 cores * 3.9 GHz | 12 | 500 | 800 |

**Table 2:** Recommended Hardware Parameters for Virtual Machine

| Category | Recommended Hardware Parameters | | | | Comment |
|---|---|---|---|---|---|
| | CPU | | Memory (GB) | Hardware Disk (GB) | |
| A | PC | Core i3 with 2 cores, 4 threads, and 3.0 GHz or higher clock speed | 4+4*number of virtual machines | 160 | The CPU of this PC supports up to two virtual machines. The CPU of this server supports up to four virtual machines. |
| | Server | Xeon E3 with 4 cores, 8M cache, and 3.0 GHz or higher clock speed | | | |
| B | PC | Core i3 with 2 cores, 4 threads, and 3.0 GHz and higher clock speed | 4+6* number of virtual machines | 280 | The CPU of this PC supports up to one virtual machine. The CPU of this server supports up to two virtual machines. |
| | Server | Xeon E3 with 4 cores, 8M cache, and 3.0 GHz or higher clock speed | | | |
| C | PC | Core i5 with 4 cores and 3.0GHz or higher clock speed | 4+10 | 450 | The CPU of this PC and server supports one virtual machine. |
| | Server | Xeon E3 with 4 cores, 8M cache, and 3.0 GHz or higher clock speed | | | |
| D | PC | i7-4770k with 4 cores, 3.5GHz clock speed, and 3.9GHz max turbo frequency | 4+12 | 500 | The CPU of this PC and server supports one virtual machine. |
| | Server | Xeon E5-2643 v2 with 6 cores, 3.5 GHz clock speed, and 3.8 GHz max turbo frequency | | | |

**Table 3:** Recommended Hardware Parameters for PC or Server

## Unified Intelligence System Software

Copy the installation file of the unified intelligence system software from the disk to the machine with the VMware vSphere Client installed. For different product models of Hillstone devices, Hillstone provides with different installation files, namely OVF template files. When copying the OVF template files, make sure that you copy them to the same directory.

| Product Models | OVF Template Files |
|---|---|
| SG-6000-X5100<br>SG-6000-G6100<br>SG-6000-G5150<br>SG-6000-G3150<br>SG-6000-G2120<br>SG-6000-G2110<br>SG-6000-M6860<br>SG-6000-M6560<br>SG-6000-M6115<br>SG-6000-M6110<br>SG-6000-M3600<br>SG-6000-M3108<br>SG-6000-M3105<br>SG-6000-M3100<br>SG-6000-M2600<br>SG-6000-M2105<br>SG-6000-M1600 | SG6000-UIF-5.5R1-disk1.vmdk<br>SG6000-UIF-5.5R1.ovf<br>SG6000-UIF-5.5R1.mf |
| SG-6000-M8860<br>SG-6000-M8260<br>SG-6000-M7860<br>SG-6000-M7360<br>SG-6000-M7260 | SG6000-UIF-2-5.5R1-disk1.vmdk<br>SG6000-UIF-2-5.5R1.ovf<br>SG6000-UIF-2-5.5R1.mf |
| SG-6000-E5960<br>SG-6000-E5760<br>SG-6000-E5660<br>SG-6000-E5560<br>SG-6000-E5260<br>SG-6000-E3960<br>SG-6000-E3660<br>SG-6000-E2800<br>SG-6000-E2300<br>SG-6000-E1700<br>SG-6000-E1600 | SG6000-UIF-3-5.5R1-disk1.vmdk<br>SG6000-UIF-3-5.5R1.ovf<br>SG6000-UIF-3-5.5R1.mf |

**Table 4:** OVF Template Files for Different Product Models

## Hillstone Device, Firmware, and License

Copy the firmware from the disk to the management PC. For different product models of Hillstone devices, Hillstone provides with different firmware.

| Product Models | Firmware |
|---|---|
| SG-6000-X5100<br>SG-6000-G6100<br>SG-6000-G5150<br>SG-6000-G3150<br>SG-6000-G2120<br>SG-6000-G2110 | SG6000-UIF-5.5R1.bin |

| Product Models | Firmware |
|---|---|
| SG-6000-M6860<br>SG-6000-M6560<br>SG-6000-M6115<br>SG-6000-M6110<br>SG-6000-M3600<br>SG-6000-M3108<br>SG-6000-M3105<br>SG-6000-M3100<br>SG-6000-M2600<br>SG-6000-M2105<br>SG-6000-M1600 | |
| SG-6000-M8860<br>SG-6000-M8260<br>SG-6000-M7860<br>SG-6000-M7360<br>SG-6000-M7260 | SG6000-UIF-2-5.5R1.bin |
| SG-6000-E5960<br>SG-6000-E5760<br>SG-6000-E5660<br>SG-6000-E5560<br>SG-6000-E5260<br>SG-6000-E3960<br>SG-6000-E3660<br>SG-6000-E2800<br>SG-6000-E2300<br>SG-6000-E1700<br>SG-6000-E1600 | SG6000-UIF-3-5.5R1.bin |

**Table 5:** Firmware for Different Product Models

To obtain the license for the unified intelligence service, contact Hillstone agent. After obtaining the license file, copy it to the management PC.

## Routing Requirements

Hillstone device communicates with the virtual machine over IP. The routing between the Hillstone device and the virtual machine must be reachable. You can use the routing mode or the transparent mode to deploy your environment. NAT mode is not supported.

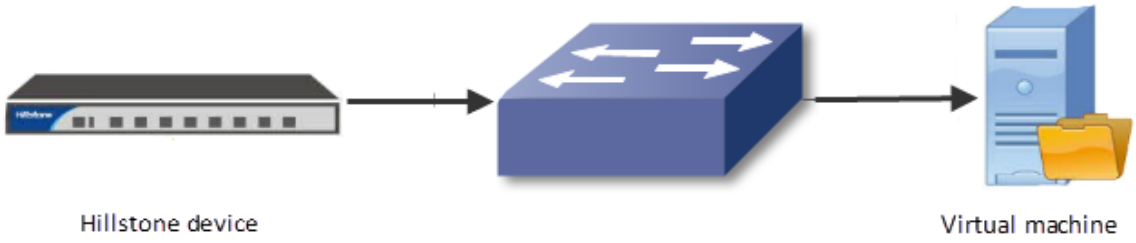


**Figure 2:** Transparent Mode

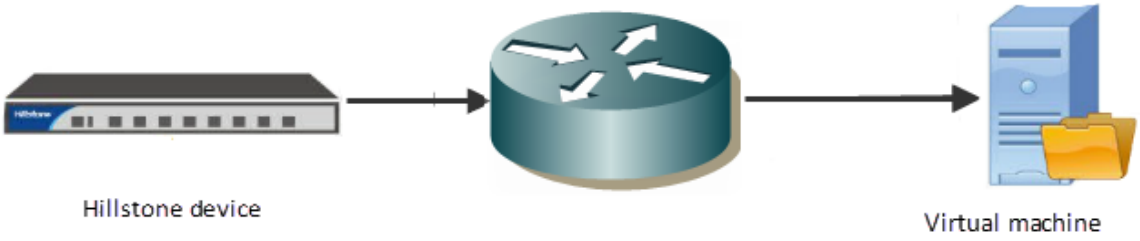


**Figure 3:** Routing Mode

# Chapter 3 Installation and Upgrading

This chapter introduces the following contents:

- Install unified intelligence system software in a virtual machine
- Upgrade Hillstone device to the specified firmware

Before executing the installation and upgrading, note the following matters:

- Ensure the unified intelligence system software and firmware have the same version number. If the version number does not match, Hillstone device cannot integrate with the virtual machine.
- If StoneOS is lower than 5.0R1, you must clear the configurations of security policy before the upgrading. After the upgrading, you need to re-configure the security policy. If StoneOS is equal to or higher than 5.0R1, the configurations of security policy will be saved during the upgrading and take effect automatically after the upgrading.
- Partial functions are not supported after the upgrading. Table 6 lists the functions that will not be supported after the upgrading and it also lists the actions performed to the configurations of these functions. For some functions, you must manually delete the corresponding configurations before the upgrading, which can avoid the conflict with the configurations of unified intelligence firewall. Hillstone recommends that you back up all configurations of StoneOS before the upgrading.

| Function | Actions to Corresponding Configurations | Comment |
|---|---|---|
| QoS | Clear the configurations | After the upgrading, use the iQoS function provided by unified intelligence firewall. You need to re-configure the settings of iQoS. |
| 802.1x | Save the global configurations;<br>Clear the configurations under the interface | N/A |
| Role | Save the configurations | To avoid the conflict with the configurations of unified intelligence firewall, you must manually delete the configurations. |
| Connect to HSM | Save the configurations | N/A |

| Function | Actions to Corresponding Configurations | Comment |
|---|---|---|
| Stat-set | Clear the configurations | After the upgrading, use the Monitor function provided by unified intelligence firewall. You need to re-configure the settings of Monitor. |
| Object (predefined URL database, user-defined URL database, URL lookup, keyword category, SSL proxy, warning page, Bypass domain, user exception) | Save the configurations | To avoid the conflict with the configurations of unified intelligence firewall, you must manually delete the configurations. |
| URL filter | | |
| URL keyword | | |
| Web posting | | |
| Email filter | | |
| IM control | | |
| HTTP/FTP control | | |
| Black lists | | |
| HA | | |
| VSYS | | |
| IPv6 | Clear the configurations | N/A |
| AV and IPS | Save the configurations | To avoid the conflict with the configurations of unified intelligence firewall, you must manually delete the configurations. After the upgrading, use the Threat Protection function provided by the unified intelligence firewall. You need to re-configure the settings of Threat Protectoin. |

**Table 6:** Unsupported Functions after Upgrading

To use the iQoS and Threat Protection functions provided by unified intelligence firewall, you need to apply for the corresponding licenses by contacting Hillstone agent.

# Installing Unified Intelligence System Software

To install unified intelligence system software, take the following steps:

1. Start VMware vSphere Client.
2. Enter the corresponding IP address/name, username, and password.

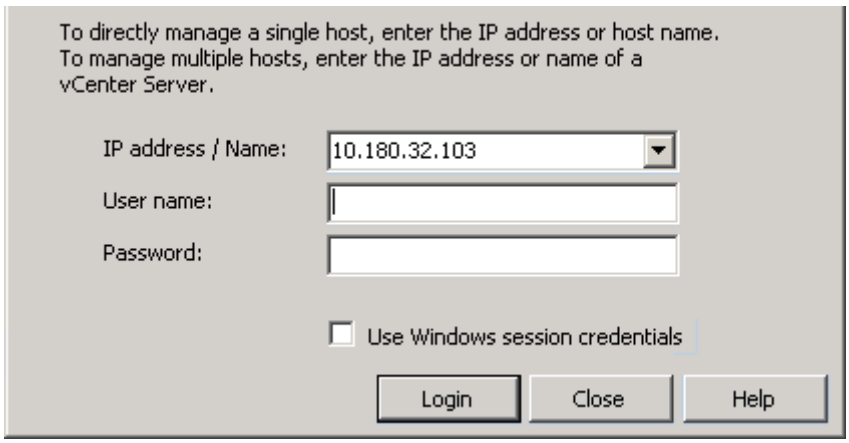
To directly manage a single host, enter the IP address or host name.
To manage multiple hosts, enter the IP address or name of a vCenter Server.
IP address / Name:
10.180.32.103
User name:
Password:
Use Windows session credentials
Login
Close
Help

**Figure 4:** Entering Required Information

3. Click **Login**. The main page of vSphere Client appears.
4. Select a host where you want to install the unified intelligence system software.

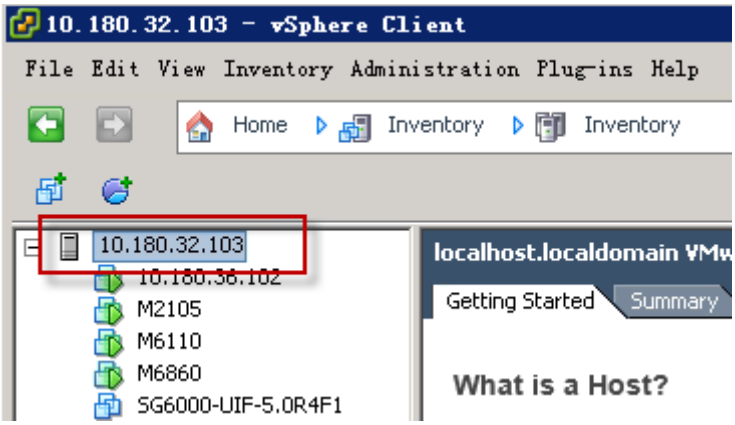


**Figure 5:** Selecting a Host

5. In the menu, click **File > Deploy OVF Template**. The **Deploy OVF Template** window appears.

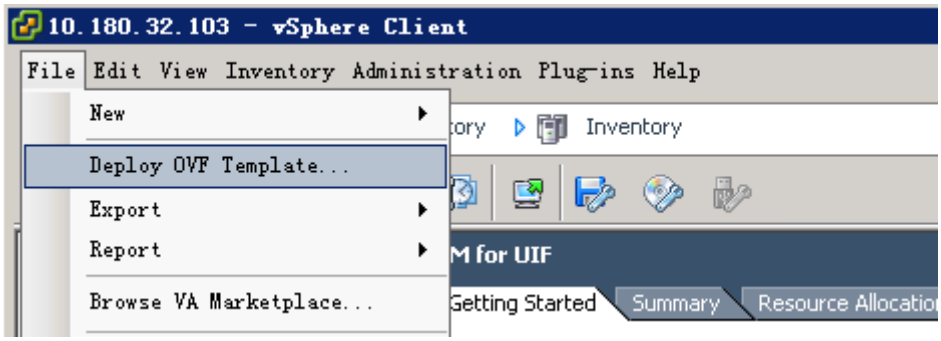


**Figure 6:** Clicking Deploy OVF Template

6. In the **Deploy OVF Template** window, click **Browse**. Then select the OVF file in the pop-up window. Note that you must select the right OVF file according to your product model. For information about OVF file selection, see Table 4.

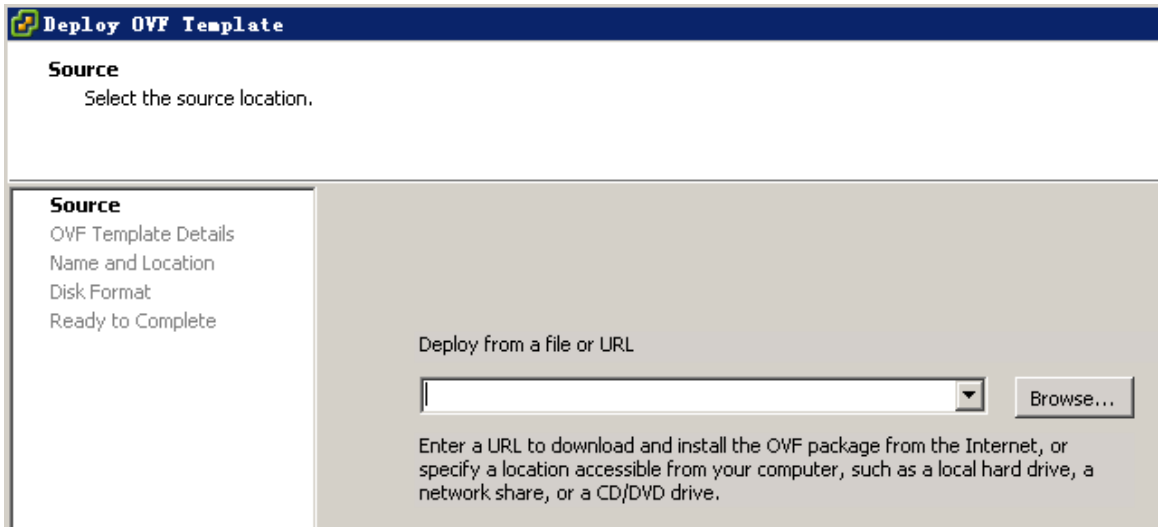
Deploy OVF Template
Source
Select the source location.
Source
OVF Template Details
Name and Location
Disk Format
Ready to Complete
Deploy from a file or URL
Browse...
Enter a URL to download and install the OVF package from the Internet, or specify a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

**Figure 7:** Clicking Browse to Select OVF File

7. After selecting the OVF file, click **Next**. The **OVF Template Details** page appears.
8. View details and then click **Next**. The **Name and Location** page appears.

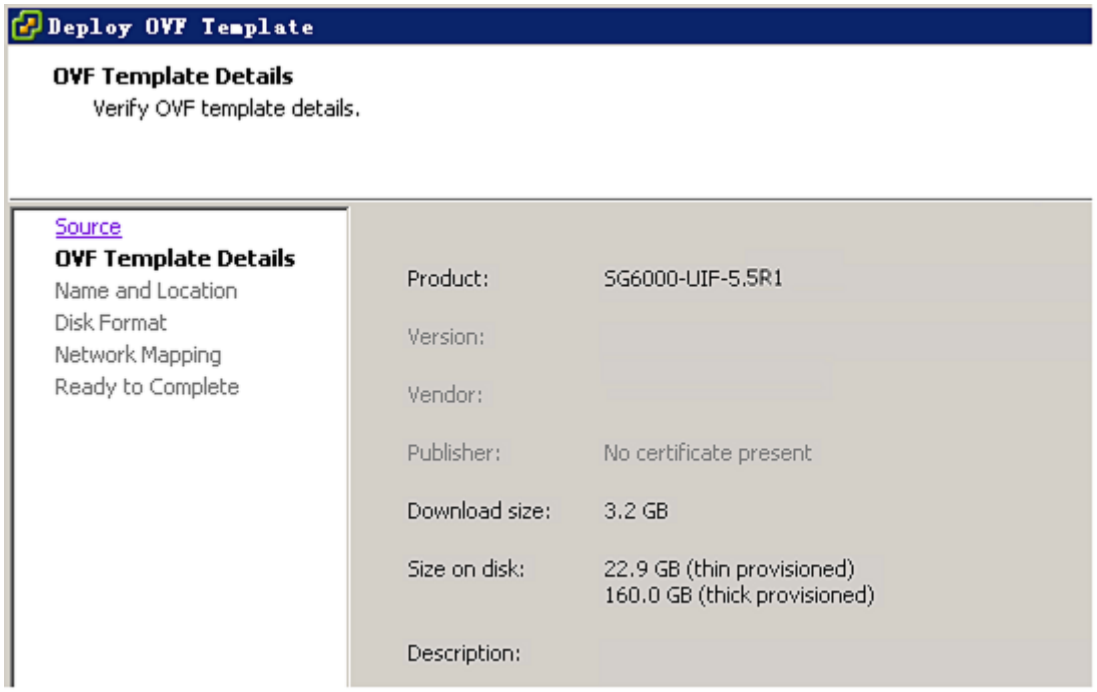


**Figure 8:** Viewing OVF Template Details

9. In the **Name and Location** page, specify a name for the deployed template. Then click **Next**. The **Disk Format** page appears.

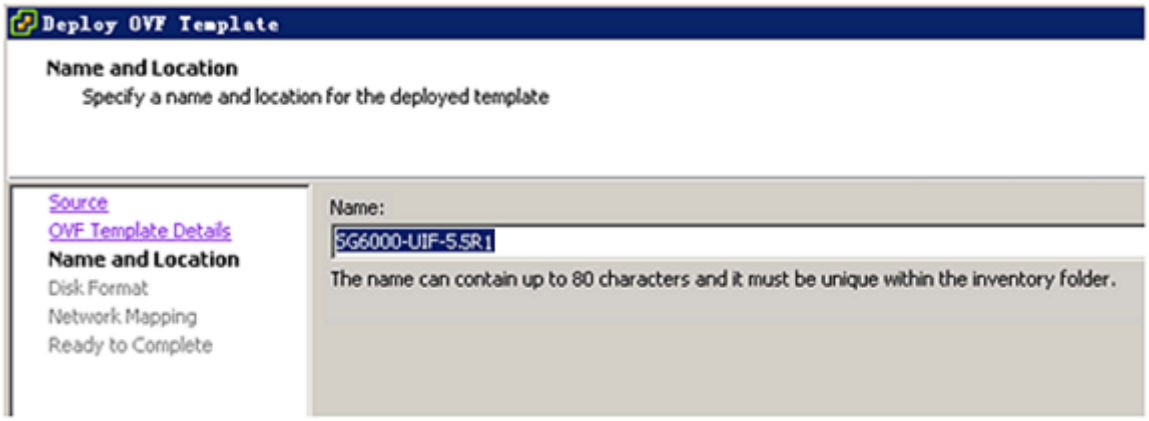
Deploy OVF Template
Name and Location
Specify a name and location for the deployed template
Source
OVF Template Details
Name and Location
Disk Format
Network Mapping
Ready to Complete
Name:
SG6000-UIF-5.5R1
The name can contain up to 80 characters and it must be unique within the inventory folder.

**Figure 9:** Specifying a Name

10. In the **Disk Format** page, select **Thick Provision Lazy Zeroed** or **Thick Provision Eager Zeroed**. Both formats are supported by unified intelligence system software. Then click **Next**. The **Network Mapping** page appears.

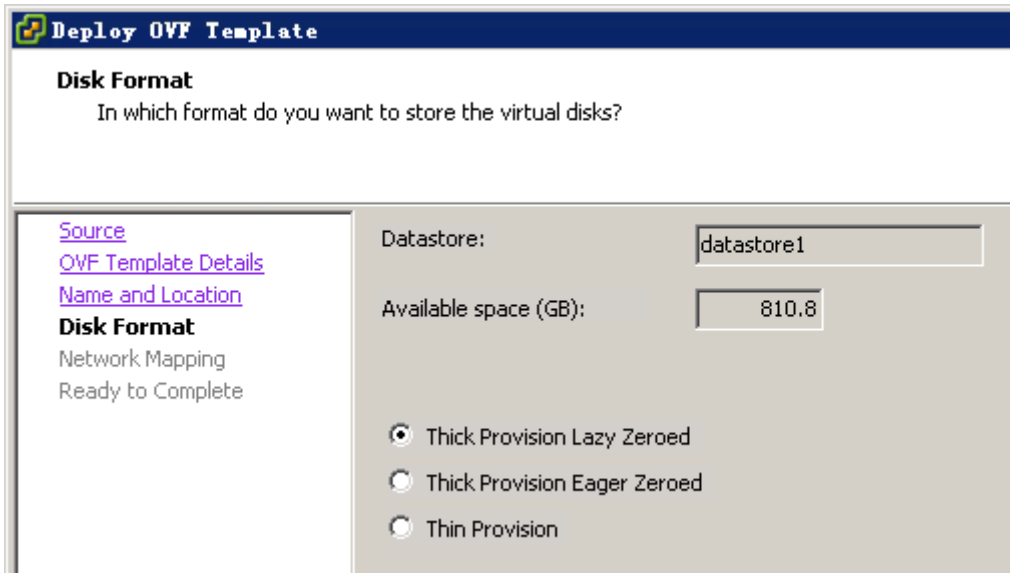


**Figure 10:** Selecting a Disk Format

11. In the **Network Mapping** page, map the networks used in the OVF template to networks in you inventory. Then click **Next**. The **Ready to Complete** page appears.

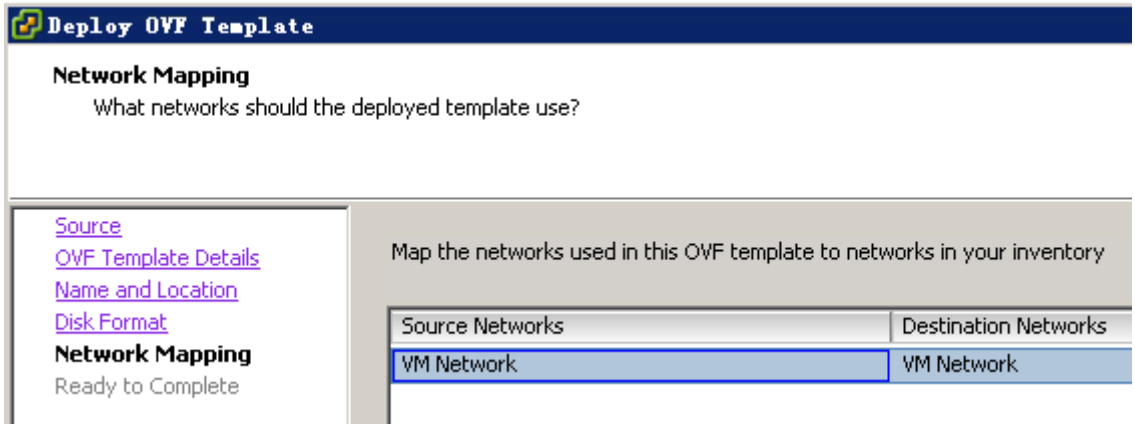


**Figure 11:** Configuring Network Mapping Settings

12. In the **Ready to Complete** page appears, verify the configured options. After you click **Finish**, the deployment task will be started.

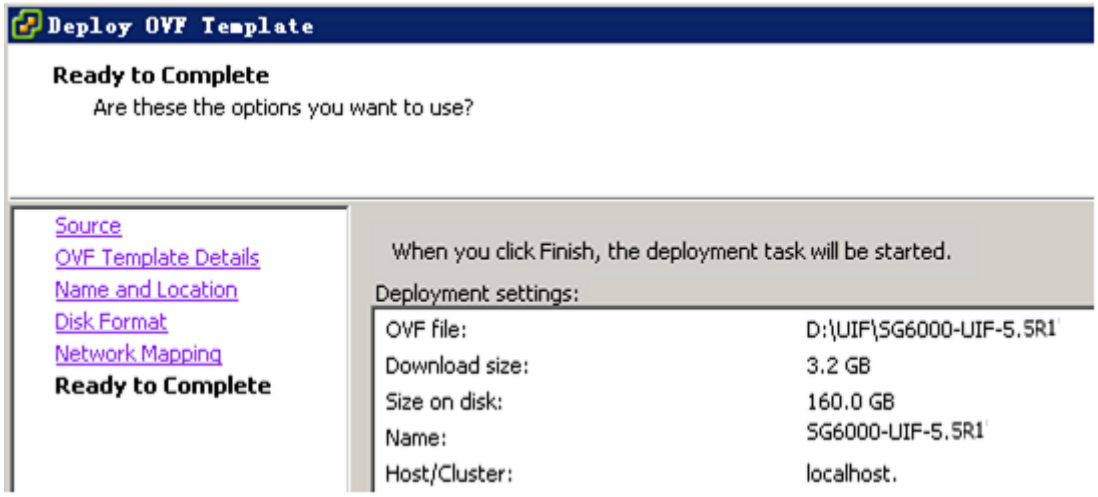


**Figure 12:** Verifying Configuration Options

13. Click **Finish** to start the deployment task. The Deploying SG6000-UIF-5.5R1 dialog appears.

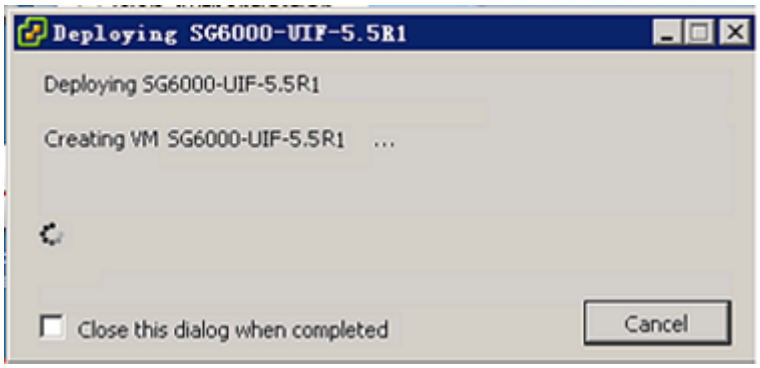


**Figure 13:** Deployment Task

14. After successfully deploying the OVF template, right-click the virtual machine where the OVF template is deployed and select **Edit Settings** from the pop-u menu. The **Virtual Machine Properties** page appears.

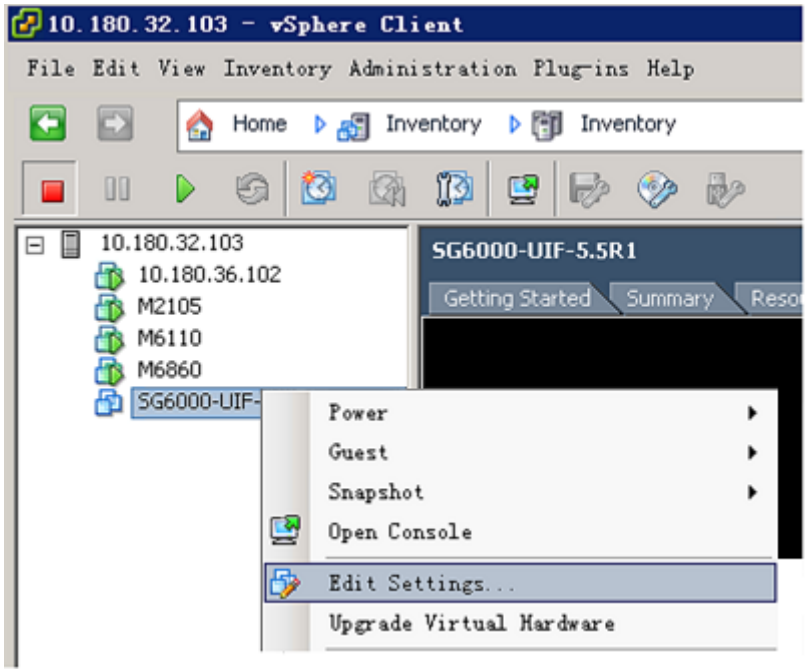


**Figure 14:** Selecting Edit Settings

15. With the **Hardware** tab active, configure the memory and hard disk according to the recommendations in Table 2.

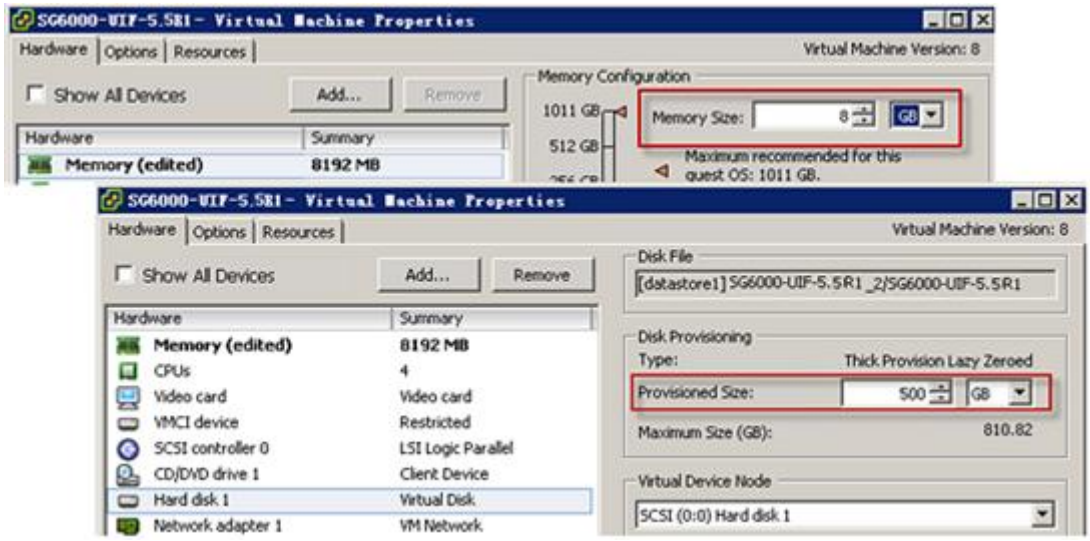


**Figure 15:** Configuring Memory Size and Disk Provisioning Size

16. With the **Resources** tab, configure the reservation of CPU according to the recommendations in the following table.

| Category | CPU Reservation |
|---|---|
| A | 3.2 GHz |
| B | 4.8 GHz |
| C | 10.0 GHz |
| D | 15.6 GHz |

**Table 7:** Configuring CPU Reservation

After completing the deployment task, the unified intelligence system software is installed. Power on your virtual machine and wait for several minutes. Then the login page appears as shown below.

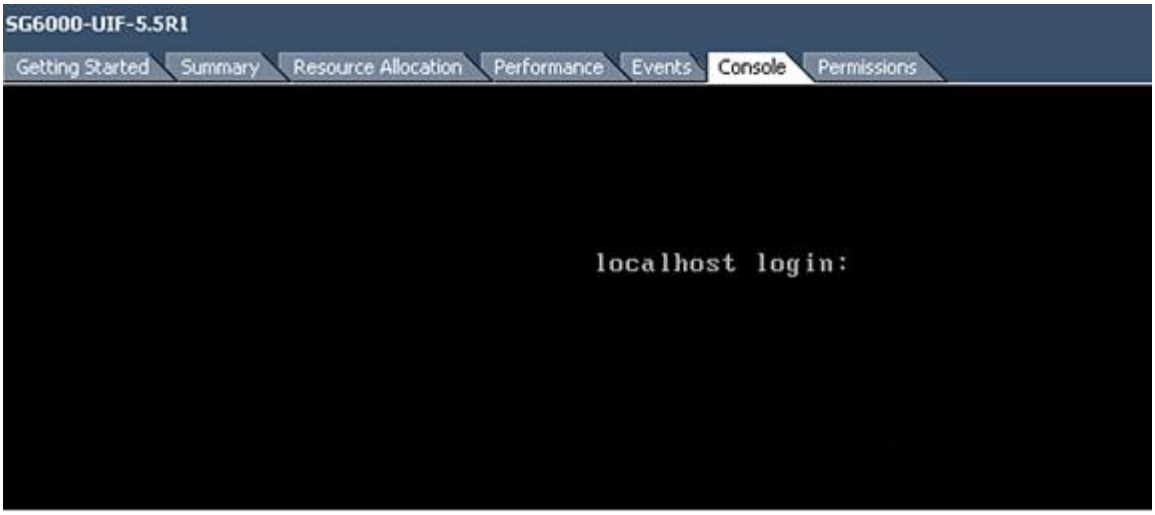


**Figure 16:** Login Page Appears

To ensure the security of the virtual machine where the unified intelligence system software locates, Hillstone sets the following limitations:

- Only the following ports of TCP are available: 21, 22, 23, 80, 443, 9091, 9092, and 9098.
- Only the following ports of UDP are available: 514 and 4739.

## Upgrading Hillstone Device

You can upgrade Hillstone device to the specified firmware via WebUI or CLI. The steps below describe the upgrading via WebUI.

1. Log into the WebUI of Hillstone device.
2. Navigate to **System > Firmware Management**. The **Upgrade Wizard** window appears.
3. Select **Upgrade to a new version** and then click **Next**.
4. Select the backup version from the drop-down list.
5. Click **Browse** and select the firmware. Note that you must select the correct firmware according to your product model. For information about firmware selection, see Table 5.
6. Click **Upgrade**. Hillstone device starts upgrading.
7. After successfully upgrading the device, click **OK**.

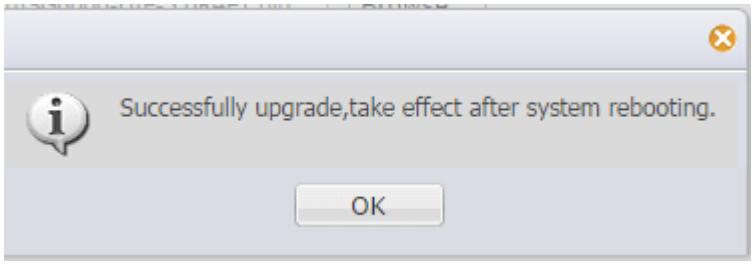


**Figure 17:** Clicking OK

8. In the **Upgrade Wizard** window, select **Yes, reboot immediately** and click **OK** to reboot the device immediately. After the reboot, the firmware takes effect.

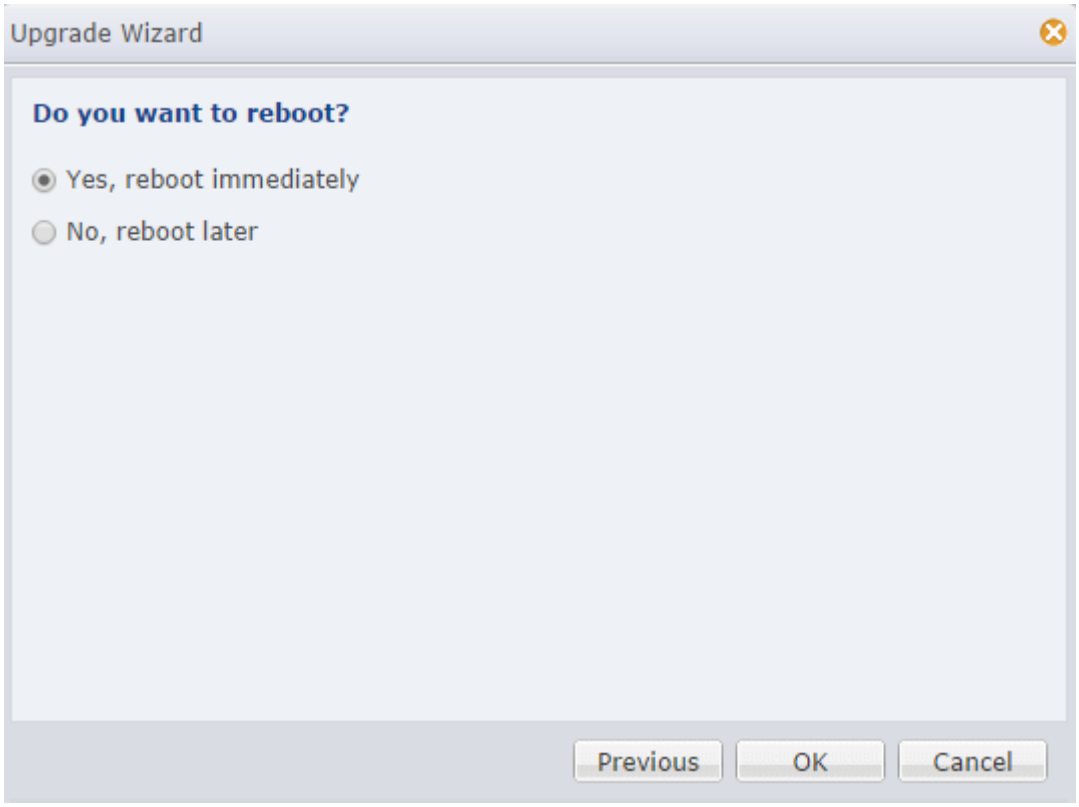


**Figure 18:** Clicking OK to Reboot

# Chapter 4 Initialization

After installing the unified intelligence system software into the virtual machine and upgrading the Hillstone device to the specified firmware, you need to proceed to perform the initialization. The initialization contains the following works:

Works executed in the virtual machine

- Set the product model and its SN
- Configure the network settings for the unified intelligence system
- (Optional) Configure the trusted devices

Works executed in the Hillstone device

- Import the license for unified intelligence service
- Connect the Hillstone device with the unified intelligence system

## Works Executed in Virtual Machine

This section describe the following works executed in the virtual machine:

- Set the product model and its SN
- Configure the network settings for the unified intelligence system
- (Optional) Configure the trusted devices

Take the following steps to execute the works:

1. With the login page of unified intelligence system active, enter the credentials and then press **Enter**.
   - Username: hillstone
   - Password: hillstone
2. The initialization wizard starts. Enter the product model. For example, if the product model of your device is SG-6000-M3108, you only need to enter M3108. Then press **Enter**.

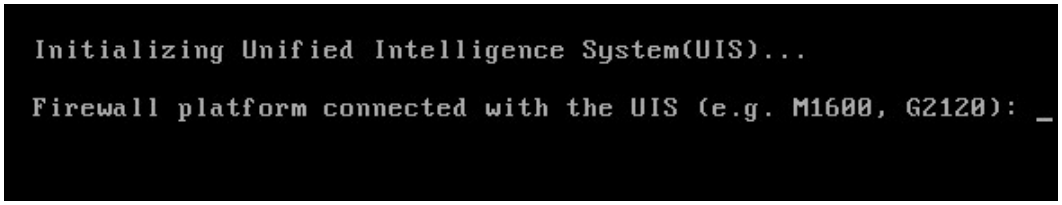


**Figure 19:** Entering Product Model

3. Enter the serial number of your Hillstone device. Then press **Enter**. The unified intelligence system will check the hardware parameters of the current virtual

machine according to the product model and serial number. You can adjust the hardware parameters according to the warning information.

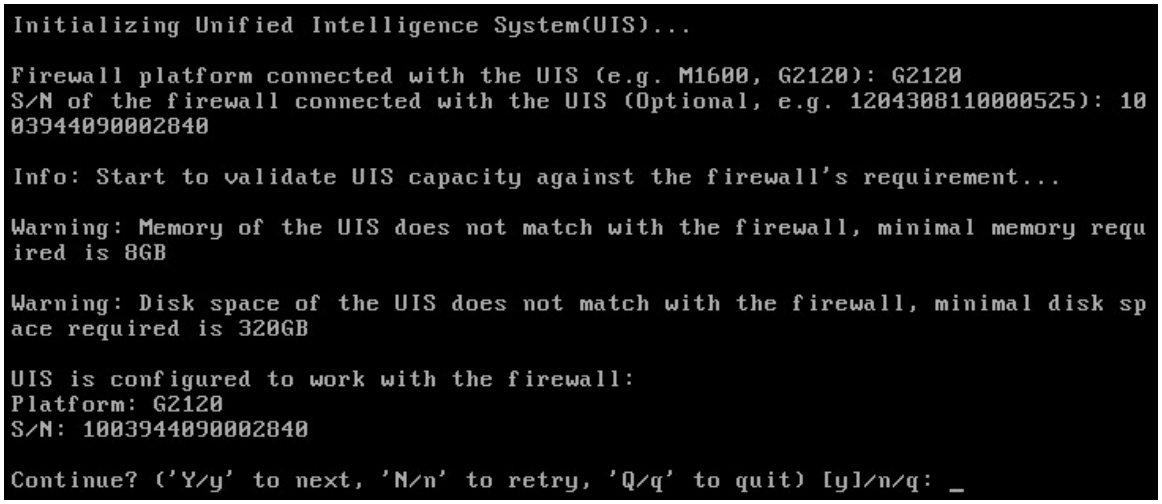
Initializing Unified Intelligence System(UIS)...
Firewall platform connected with the UIS (e.g. M1600, G2120): G2120
S/N of the firewall connected with the UIS (Optional, e.g. 1204308110000525): 10
03944090002840
Info: Start to validate UIS capacity against the firewall's requirement...
Warning: Memory of the UIS does not match with the firewall, minimal memory requ
ired is 8GB
Warning: Disk space of the UIS does not match with the firewall, minimal disk sp
ace required is 320GB
UIS is configured to work with the firewall:
Platform: G2120
S/N: 1003944090002840
Continue? ('Y/y' to next, 'N/n' to retry, 'Q/q' to quit) [y]/n/q: _

**Figure 20:** Entering Serial Number and Checking Hardware Parameters

4. Enter **Y** and then press **Enter**. The wizard goes to the network configuration. To change the product model and serial number, enter **N** and press **Enter**. To exit the wizard, enter **Q** and press **Enter**.

5. In the network configuration, specify the IP address, netmask, gateway (optional) of the unified intelligence system's interface according to your requirements. Then press **Enter**. The unified intelligence system will check the configurations.

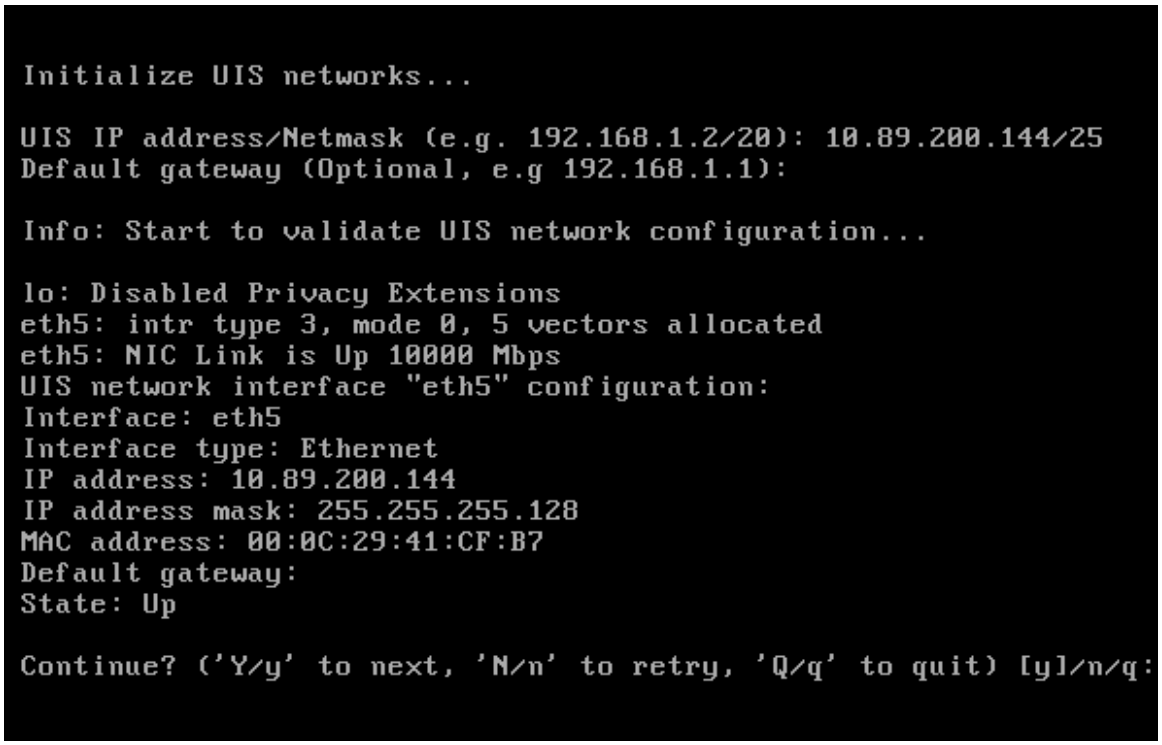
Initialize UIS networks...
UIS IP address/Netmask (e.g. 192.168.1.2/20): 10.89.200.144/25
Default gateway (Optional, e.g 192.168.1.1):
Info: Start to validate UIS network configuration...
lo: Disabled Privacy Extensions
eth5: intr type 3, mode 0, 5 vectors allocated
eth5: NIC Link is Up 10000 Mbps
UIS network interface "eth5" configuration:
Interface: eth5
Interface type: Ethernet
IP address: 10.89.200.144
IP address mask: 255.255.255.128
MAC address: 00:0C:29:41:CF:B7
Default gateway:
State: Up
Continue? ('Y/y' to next, 'N/n' to retry, 'Q/q' to quit) [y]/n/q:

**Figure 21:** Configuring Network Settings

6. Enter **Y** and then press **Enter**. The wizard goes to the trusted devices configuration. To change the network configuration, enter **N** and press **Enter**. To exit the wizard, enter **Q** and press **Enter**.
7. In the trusted devices configuration, specify the IP address and netmask. If you specify the IP address and netmask, only the Hillstone device with the specified configuration can connect with the unified intelligence system. If not, any Hillstone device can connect with the unified intelligence system. Then press **Enter**. The unified intelligence system will check the configurations.
8. Enter **Y** and then press **Enter**. The initialization is completed. To change the trusted devices configuration, enter **N** and press **Enter**. To exit the wizard, enter **Q** and press **Enter**.

# Works Executed in Hillstone Device

This section describes the following works executed in the Hillstone device.

- Import the license for unified intelligence service. After you import the license to the Hillstone device and restart the device, it will support the unified intelligence service.
- Connect the Hillstone device with the unified intelligence system. To establish the connection, you need to ensure that the routing between the Hillstone device and the virtual machine is reachable and configure the corresponding settings. After successfully connecting the Hillstone device with the unified intelligence system, they can automatically check the connection status and re-connect if the connection is disconnected.

You can complete the works above via WebUI or via CLI.

## Via WebUI

Perform the followings operations via WebUI:

1. Login into the WebUI of Hillstone device. For example, http://10.160.36.122/
2. Click **System > License** to install the license for unified intelligence service. You can click **Browse** to upload the license file or manually input the license string.
3. Click **System > Unified Intelligence System** to configure the interface for connecting with the unified intelligence system.
   - IP Address of UIS: Enter the IP address of the unified intelligence system.
   - Virtual Router: From the drop-down box, select the virtual router for connecting with the unified intelligence system.
   - UIS Status: Display the connection status.
4. Click **OK**. Wait for the connection establishment process. Establishing the connection may take several minutes. You can view the connection status in the UIS status section.

**Figure 22:** Viewing Connection Status

**Note:** The unified intelligence system can keep connected with only one Hillstone device. When the unified intelligence system has connected with a Hillstone device, it will refuse connection requests from other Hillstone devices.

## Via CLI

Perform the following operations via CLI:

1. Login into the CLI of the Hillstone device.
2. In any mode, use the following command to import the license:

   **exec license install** *license-string*
3. After successfully importing the license, enter the configuration mode and configure the settings for establishing the connection:

   **apm** *ip-address* [**vrouter** *vrouter-name*]

   - *ip-address* – Enter the IP address of the virtual machine with the unified intelligence system installed.
   - **vrouter** *vrouter-name* – Enter the vrouter that the interface belongs to. If you do not specify the vrouter, the default vrouter trust-vr will be used.
4. Wait for the connection establishment process. Establishing the connection may take several minutes. You can enter the following command to view the connection status:

   **show apm destination**

   - If the value of the **Application module status** property is **connecting**, the Hillstone device is try to connect with the unified intelligence system.
   - If the value of the **Application module status** property is **connected**, the Hillstone device connects with the unified intelligence system.

```
SG-6000# show apm destination
Application module parameters:
------------------------------------------------------------
Application module IP address:          10.180.186.19
Application module vrouter:             trust-vr
Application module service port:        9098
Application module status:              connected
Application module share key:           YES
------------------------------------------------------------
```

**Figure 23:** Viewing Connection Status

**Note:** The unified intelligence system can keep connected with only one Hillstone device. When the unified intelligence system has connected with a Hillstone device, it will refuse connection requests from other Hillstone devices.

# Chapter 5 Logging into Unified Intelligence Firewall

After successfully establishing the connection, you can use the unified intelligence firewall. To log into the unified intelligence firewall, take the following steps:

1. Enter the IP address of the interface in your Web browser. For example, http://10.160.36.122/. The login page appears.
2. Enter the credentials and then click **Login**.
    - Username: hillstone
    - Password: hillstone

For more information about using the unified intelligence firewall, see *StoneOS WebUI User Guide*.

# Chapter 6 Advanced Settings

You can configure the advanced settings for the unified intelligence firewall.

## Showing Interface Information

Log into the CLI of the unified intelligence system and enter the command below to view the interface information:

```
show interface
```

## Configuring Interface Settings

Log into the CLI of the unified intelligence system and enter the command below to configure the IP address and gateway of the interface:

**ip address add** *ip-address/mask* [**gateway** *ip-address*]

- *ip-address/mask* – Enter the IP address and the netmask of this interface.
- *ip-address* – Enter the IP address of the gateway.

## Modifying Login Password

Log into the CLI of the unified intelligence system and enter the command below in the global configuration mode to modify the login password:

**password** *password*

To restore the password to the original one, enter the command below in the global configuration mode:

**no password**

## Upgrading Unified Intelligence Firewall

Upgrading the unified intelligence firewall can both upgrade the unified intelligence system and the firmware of Hillstone device.

You can upgrade the unified intelligence firewall via WebUI or CLI.

### Via WebUI

To upgrade the unified intelligence firewall via WebUI, take the following steps:

1. Log into the WebUI of the unified intelligence firewall.
2. Before 5.5R1 version, navigate to **System > System Management > Upgrade Management > Firmware Upgrade**.

From 5.5R1 version, navigate to **System > Upgrade Management > Upgrade Firmware**.

3. In the Upgrade Firmware section, click **Browse** and select the .iso file from your local disk. For .iso file selection, see Table 8. As for the version from 5.5R1, backup your system configuration is recommended.

4. Select the **Reboot to make the new firmware take effect** checkbox and click **Apply** to reboot system and make the .iso file take effect.

   If you click **Apply** without selecting the checkbox, the .iso file will take effect after the next startup.

| Product Models | Firmware |
|---|---|
| SG-6000-X5100<br>SG-6000-G6100<br>SG-6000-G5150<br>SG-6000-G3150<br>SG-6000-G2120<br>SG-6000-G2110<br>SG-6000-M6860<br>SG-6000-M6560<br>SG-6000-M6115<br>SG-6000-M6110<br>SG-6000-M3600<br>SG-6000-M3108<br>SG-6000-M3105<br>SG-6000-M3100<br>SG-6000-M2600<br>SG-6000-M2105<br>SG-6000-M1600 | SG6000-UIF-5.5R1.iso |
| SG-6000-M8860<br>SG-6000-M8260<br>SG-6000-M7860<br>SG-6000-M7360<br>SG-6000-M7260 | SG6000-UIF-2-5.5R1.iso |
| SG-6000-E5960<br>SG-6000-E5760<br>SG-6000-E5660<br>SG-6000-E5560<br>SG-6000-E5260<br>SG-6000-E3960<br>SG-6000-E3660<br>SG-6000-E2800<br>SG-6000-E2300<br>SG-6000-E1700<br>SG-6000-E1600 | SG6000-UIF-3-5.5R1.iso |

**Table 8:** ISO Files for Different Product Models

### Via CLI

To upgrade the unified intelligence firewall via CLI, log into the CLI of the Hillstone device. In the execution mode, execute the following command:

**import image from ftp server ip-address [vrouter vrouter-name] user** *user-name* **password** *password file-name*

- *ip-address* – Specify the IP address of the FTP server.
- *vrouter-name* – Upgrade the specified virtual router.
- **user** *user-name* **password** *password* – Specify the IP address and username for logging into the FTP server.
- *file-name* – Enter the name of the .iso file. For .iso file selection, see Table 8.

After successfully upgrading the unified intelligence firewall, restart the Hillstone device and the virtual machine manually.

## Upgrading/Rolling Back Firmware of Hillstone Device

You can upgrade the firmware of Hillstone device, or roll back the firmware of Hillstone device.

Before rolling back the firmware of Hillstone device, you need to manually clear the settings of the threat protection function. For the functions that are both supported by Hillstone devices and unified intelligence firewall, the configurations will be rolled back and take effect after the rollback. For other functions, you need to do nothing and they will not affect the rollback. Hillstone recommends that you back up all configurations of the unified intelligence firewall before the rollback.

To perform the rollback, log into the CLI mode of the Hillstone device and execute the following command:

**import image-bfm from ftp server** *ip-address* [vrouter *vrouter-name*] **user** *user-name* **password** *password file-name*

- *ip-address* – Specify the IP address of the FTP server.
- *vrouter-name* – Upgrade/roll back the specified virtual router.
- **user** *user-name* **password** *password* – Specify the IP address and username for logging into the FTP server.
- *file-name* – When upgrading the firmware of the Hillstone device, select the firmware that has the same version number with the unified intelligence system soft. When rolling back the firmware of the Hillstone device before 5.5R1 version, specify the firmware of the common version. From 5.5R1 version, you need to uninstall the unified intelligence service license first, and then reboot the system. The system will roll back to the common version and keep the same version number with the unified intelligence system soft. For more information, see *StoneOS CLI User Guide*.

## Deleting Unified Intelligence System

To delete the unified intelligence system, you can delete the virtual machine with the unified intelligence system installed or format the disk of the virtual machine.

## Showing Version Information

To view the version information of the unified intelligence system software, log into the CLI of the unified intelligence system and execute the command below in any mode:

```
show image
```

To view the version information of the firmware of the Hillstone device, log into the CLI of the Hillstone device and execute the command below in any mode:

```
show version
```

## Configuring Trusted Hosts

You can specify the range of IP addresses and only the Hillstone device whose interface IP address is within the range can establish the connection with the unified intelligence firewall. The Hillstone device whose interface IP address is within the range is called trusted host.

To specify the range of IP addresses, log into the CLI of the unified intelligence system and execute the command below in the global configuration mode:

**trust-bfm address** *ip-address/mask*

- *ip-address/mask* – Specify the range of IP addresses.

## Securing Communication between Unified Intelligence System and Hillstone Device

Hillstone secures the communication between the unified intelligence system and the Hillstone device by using the following methods:

- Use SSL certificate to secure the TIPC data. The SSL certificates are stored in both sides.
- When establishing the connection at the first time, the unified intelligence system will generate the share key automatically and randomly. The Hillstone device requests this share key and stores it in the local. Both sides use this share key to validate the connection information.

## Viewing Share Keys

To view whether there is a share key in the local of the Hillstone device, you can log into the CLI of the Hillstone device and execute the following command:

```
show apm destination
```

In the output information, view the value of the **Application module share key** parameter. **YES** represents that there is a share key in the local of the Hillstone device. **NO** represents no share key.

```
SG-6000# show apm destination
Application module parameters:
============================================================
Application module IP address:          10.180.186.19
Application module vrouter:             trust-vr
Application module service port:        9098
Application module status:              connected
Application module share key:           YES
============================================================
```

**Figure 24:** Viewing Share Key

To view whether there is a share key in the local of the unified intelligence system, you can log into the CLI of the Hillstone device and execute the following command:

```
show bfm destination
```

In the output information, view the value of the **Basic firewall module share key** parameter. **Yes** represents that there is a share key in the local of the Hillstone device. **NO** represents no share key.

## Clearing Share Keys

When you change a new Hillstone device to connect with the unified intelligence system, you must clear the share keys in both sides.

To clear the share key in the local of the Hillstone device, you can log into the CLI of the Hillstone device and execute the following command:

```
clear apm key
```

To clear the share key in the local of the unified intelligence system, you can log into the CLI of the unified intelligence system and execute the following command:

```
clear bfm key
```

# Copyright Information

Copyright © 2014-2015, Hillstone Networks, lnc. All rights reserved.

Hillstone, Hillstone Networks logo, StoneOS, StoneManager, Hillstone PnPVPN, UTM Plus are trademarks of Hillstone Networks.

All other trademarks or registered marks are the property of their respective owners. Hillstone Networks assumes no responsibility for any inaccuracies in this document. Hillstone Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Hillstone Networks Website www.hillstonenet.com posts the latest information.